F.T. Breuer, O. Kramer, M. Stolpe Dortmund, 5. Januar 2009

Übungen zur Vorlesung

Betriebssysteme, Rechnernetze und verteilte Systeme II

Wintersemester 2008/2009

Blatt 10

Aufgabe 10.1 (4 Pkte.) Das Protokoll ap5.0 weist als Sicherheitslücke die Man-in-the-Middle-Attacke auf. Das Protokoll ap4.0 hingegen hat keine Schwachstellen, was die Authentifikation von Alice angeht. Allerdings muss Alice auch darauf achten, dass sie tatsächlich mit Bob kommuniziert.

(a) Warum ist bei Protokoll ap5.0 im Gegensatz zu ap4.0 die Man-in-the-Middle-Attacke möglich?

(b) Kann das Protokoll ap4.0 auch verwendet werden, um Bob gegenüber Alice zu authentifizieren? Begründen Sie ihre Antwort.

(c) Lässt sich die Man-in-the-Middle-Attacke bei ap5.0 vermeiden, indem sich Bob gegenüber Alice mittels ap5.0 authentifiziert? Erläutern Sie ihre Antwort.

Aufgabe 10.2 (4 Pkte.) Um kryptographische Verfahren erfolgreich einsetzen zu können, ist es notwendig, Schlüssel an die beteiligten Kommunikationspartner zu verteilen. Im Fall symmetrischer Verschlüsselung übernimmt diese Aufgabe ein KDC (Key Distribution Center). Für Public-Key-Verfahren ist die Einrichtung einer zentralen Zertifizierungsstelle (CA, Certification Authority) für die öffentlichen Schlüssel der jeweiligen Kommunikationspartner nötig.

(a) Welche Schwachstelle soll mittels Zertifizierung öffentlicher Schlüssel durch einen unbeteiligten Dritten behoben werden? Welches kryptographische Verfahren kommt dabei auf welche Weise zum Einsatz? Wozu wird der öffentliche Schlüssel der CA benötigt?

(b) Angenommen, ein Unternehmen hat sich seinen öffentlichen Schlüssel durch eine CA zertifizieren lassen. Alice möchte per SSL auf die Webseite des Unternehmes zugreifen. Um die Gültigkeit des Zertifikats überprüfen zu können, benötigt sie den öffentlichen Schlüssel der jeweiligen CA. Hierbei könnte sich ein unendlicher Regress ergeben, da unklar ist, wer die Authentizität des CA-Schlüssels bestätigen soll. Auf welche Weise muss der öffentliche Schlüssel der CA im Idealfall an Alice übermittelt werden?

(c) In der Praxis sind die öffentlichen Schlüssel von bekannten CAs bereits in der Browser-Software enthalten, die man heutzutage aus dem Internet herunterlädt und dann installiert. Warum ist diese Art der Verteilung von öffentlichen CA-Schlüsseln problematisch?

Aufgabe 10.3 (2 Pkte.) Sie beraten ein Unternehmen in Sicherheitsfragen. Das Unternehmen plant den Kauf einer Firewall.

(a) Erläutern Sie, warum der Einsatz einer Firewall unter Umstanden das Risiko eines Angriffs erhöhen kann.

(b) Welche Lösung scheint in ihren Augen die bessere zu sein: das Abschalten nicht benötigter Dienste oder eine Zugriffsbeschränkung auf nicht benötigten Diensten mit Hilfe einer Firewall? Diskutieren Sie Vor- und Nachteile der Varianten in Hinblick auf Sicherheitsrisiken und Administrationsaufwand.